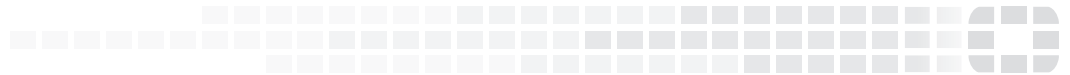


FORTINET®



FortiOS™ Handbook - Hardening your FortiGate

VERSION 5.6.3



FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FORTINET PRIVACY POLICY

<https://www.fortinet.com/corporate/about-us/privacy.html>

FEEDBACK

Email: techdocs@fortinet.com



3/21/2018

FortiOS™ Handbook - Hardening your FortiGate

01-563-467596-20180321

TABLE OF CONTENTS

Change Log	5
Introduction	6
Building security into FortiOS	7
Boot PROM and BIOS security	7
FortiOS kernel and user processes	7
Administration access security	7
Admin administrator account	7
Secure password storage	7
Maintainer account	8
Administrative access security	8
Network security	9
Network interfaces	9
TCP sequence checking	10
Reverse path forwarding	10
FIPS and Common Criteria	10
PSIRT advisories	10
FortiOS ports and protocols	11
FortiOS open ports	11
Closing open ports	14
Security best practices	15
Install the FortiGate unit in a physically secure location	15
Register your product with Fortinet Support	15
Keep your FortiOS firmware up to date	15
System administrator best practices	16
Disable administrative access to the external (Internet-facing) interface	16
Allow only HTTPS access to the GUI and SSH access to the CLI	16
Require TLS 1.2 for HTTPS administrator access	16
Re-direct HTTP GUI logins to HTTPS	16
Change the HTTPS and SSH admin access ports to non-standard ports	17
Maintain short login timeouts	17
Restrict logins from trusted hosts	17
Set up two-factor authentication for administrators	18
Create multiple administrator accounts	18
Modify administrator account lockout duration and threshold values	18

Rename the admin administrator account	19
Add administrator disclaimers	19
Global commands for stronger and more secure encryption	19
Turn on global strong encryption	20
Disable MD5 and CBC for SSH	20
Disable static keys for TLS	20
Require larger values for Diffie-Hellman exchanges	20
Disable sending Malware statistics to FortiGuard	20
Disable auto USB installation	21
Set system time by synchronizing with an NTP server	21
Enable password policies	21
Configure auditing and logging	21
Encrypt logs sent to FortiAnalyzer/FortiManager	22
Disable interfaces that not used	22
Disable unused protocols on interfaces	22
Use local-in policies to close open ports or restrict access	23
Close ICMP ports	23
Close the BGP port	24

Change Log

Date	Change Description
March 21, 2018	Updated with new information throughout.
February 15, 2018	Updated for FortiOS 5.6.3.

Introduction

This guide describes some of the techniques used to harden (improve the security of) FortiGate devices and FortiOS.

This document contains the following sections:

- [Building security into FortiOS](#)
- [FortiOS ports and protocols](#)
- [Security best practices](#)

Building security into FortiOS

The FortiOS operating system, FortiGate hardware devices, and FortiOS virtual machines (VMs) are built with security in mind, so many security features are built into the hardware and software. Fortinet maintains an ISO:9001 certified software and hardware development processes to ensure that FortiOS and FortiGate products are developed in a secure manner

Boot PROM and BIOS security

The boot PROM and BIOS in FortiGate hardware devices use Fortinet's own FortiBootLoader that is designed and controlled by Fortinet. FortiBootLoader is a secure, proprietary BIOS for all FortiGate appliances. FortiGate physical devices always boot from FortiBootLoader.

FortiOS kernel and user processes

FortiOS is a multi-process operating system with kernel and user processes. The FortiOS kernel runs in a privileged hardware mode while higher-level applications run in user mode. FortiOS is a closed system that does not allow the loading or execution of third-party code in the FortiOS user space. All non-essential services, packages, and applications are removed.

FortiGate appliances with SD drives are encrypted to prevent unauthorized access to data.

Administration access security

This section describes FortiOS and FortiGate administration access security features.

Admin administrator account

All FortiGate firewalls ship with a default administrator account called admin. By default, this account does not have a password. FortiOS allows administrators to add a password for this account or to remove the account and create new custom super_admin administrator accounts.

For more information, see [Rename the admin administrator account on page 19](#).

Secure password storage

User and administrator passwords are stored securely on the system in an encrypted format. The encryption hash used for admin account passwords is SHA256/SHA1. The value that is seen in the configuration file is the Base64 encoded hash value. For example:

```
config system admin
  edit "admin"
    set accprofile "super_admin"
    set vdom "root"
```

```
set password ENC SH2n1Sm9QL9tapcHPXIqAXvX7vBJuuqu22hpa0JX0sBuKIo7z2g0Kz/+0KyH4E=  
next  
end
```

Pre-shared keys in IPSec phase-1 configurations are stored in plain text. In the configuration file these pre-shared keys are encoded. The encoding consists of encrypting the password with a fixed key using DES (AES in FIPS mode) and then Base64 encoding the result.

Maintainer account

Administrators with physical access to a FortiGate appliance can use a console cable and a special administrator account called maintainer to log into the CLI. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password for the maintainer account is bcpb followed by the FortiGate serial number. An administrator has 60-seconds to complete this login. See [Resetting a lost Admin password](#) on the Fortinet Cookbook for details.

The only action the maintainer account has permissions to perform is to reset the passwords of super_admin accounts. Logging in with the maintainer account requires rebooting the FortiGate. FortiOS generates event log messages when you login with the maintainer account and for each password reset.

The maintainer account is enabled by default; however, there is an option to disable this feature. The maintainer account can be disabled using the following command:

```
config system global  
  set admin-maintainer disable  
end
```



If you disable this feature and lose your administrator passwords you will no longer be able to log into your FortiGate.

Administrative access security

Secure administrative access features:

- SSH, Telnet, and SNMP are disabled by default. If required, these admin services must be explicitly enabled on each interface from the GUI or CLI.
- SSHv1 is disabled by default. SSHv2 is the default version.
- SSLv3 and TLS1.0 are disabled by default. TLSv1.1 and TLSv1.2 are the SSL versions enabled by default for HTTPS admin access.
- HTTP is disabled by default, except on dedicated MGMT, DMZ, and predefined LAN interfaces. HTTP redirect to HTTPS is enabled by default.
- The `strong-crypto` global setting is enabled by default and configures FortiOS to use strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH/TLS/SSL functions.
- SCP is disabled by default. Enabling SCP allows downloading the configuration file from the FortiGate as an alternative method of backing up the configuration file. To enable SCP:

```
config system global  
  set admin-scp enable  
end
```

- DHCP is enabled by default on the dedicated MGMT interface and on the predefined LAN port (defined on some FortiGate models).

- On FortiGate models with dedicated MGMT interfaces, dedicated DMZ interfaces, dedicated WAN interfaces, and pre-defined LAN interfaces, the default management access on interfaces is shown below. Outside of the interfaces listed below, management access must be explicitly enabled on interfaces – management services are enabled on specific interfaces and not globally.
 - Dedicated Management Interface
 - Ping
 - FMG-Access (fgfm)
 - CAPWAP
 - HTTPS
 - HTTP
 - Dedicated WAN1/WAN2 Ports
 - Ping
 - FMG-Access (fgfm)
 - Dedicated DMZ Port
 - Ping
 - FMG-Access (fgfm)
 - CAPWAP
 - HTTPS
 - HTTP
 - Pre-Defined LAN Port
 - Ping
 - FMG-Access (fgfm)
 - CAPWAP
 - HTTPS
 - HTTP

Network security

This section describes FortiOS and FortiGate network security features.

Network interfaces

The following are disabled by default on each FortiGate interface:

- Broadcast forwarding
- STP forwarding
- VLAN forwarding
- L2 forwarding
- Netbios forwarding
- Ident accept

For more information, see [Disable unused protocols on interfaces on page 22](#).

TCP sequence checking

FortiOS uses TCP sequence checking to ensure a packet is part of a TCP session. By default, anti-replay protection is strict, which means that if a packet is received with sequence numbers that fall out of the expected range, FortiOS drops the packet. Strict anti-replay checking performs packet sequence checking and ICMP anti-replay checking with the following criteria:

- The SYN, FIN, and RST bit cannot appear in the same packet.
- FortiOS does not allow more than 1 ICMP error packet to go through before it receives a normal TCP or UDP packet.
- If FortiOS receives an RST packet, FortiOS checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect.
- For each new session, FortiOS checks to determine if the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value.

Reverse path forwarding

FortiOS implements a mechanism called Reverse Path Forwarding (RPF), or Anti Spoofing, to block an IP packet from being forwarded if its source IP does not:

- belong to a locally attached subnet (local interface), or
- be in the routing domain of the FortiGate from another source (static route, RIP, OSPF, BGP).

If those conditions are not met, FortiOS silently drops the packet.

FIPS and Common Criteria

FortiOS has received NDPP, EAL2+, and EAL4+ based FIPS and Common Criteria certifications. Common Criteria evaluations involve formal rigorous analysis and testing to examine security aspects of a product or system. Extensive testing activities involve a comprehensive and formally repeatable process, confirming that the security product functions as claimed by the manufacturer. Security weaknesses and potential vulnerabilities are specifically examined during an evaluation.

To see Fortinet's complete history of FIPS/CC certifications go to the following URL and add Fortinet to the Vendor field:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>

PSIRT advisories

The FortiGuard Labs Product Security Incident Response Team (PSIRT) continually tests and gathers information about Fortinet hardware and software products, looking for vulnerabilities and weaknesses. Any such findings are fed back to Fortinet's development teams and serious issues are described along with protective solutions. The PSIRT regulatory releases PSIRT advisories when issues are found and corrected. Advisories are listed at <https://www.fortiguards.com/psirt>.

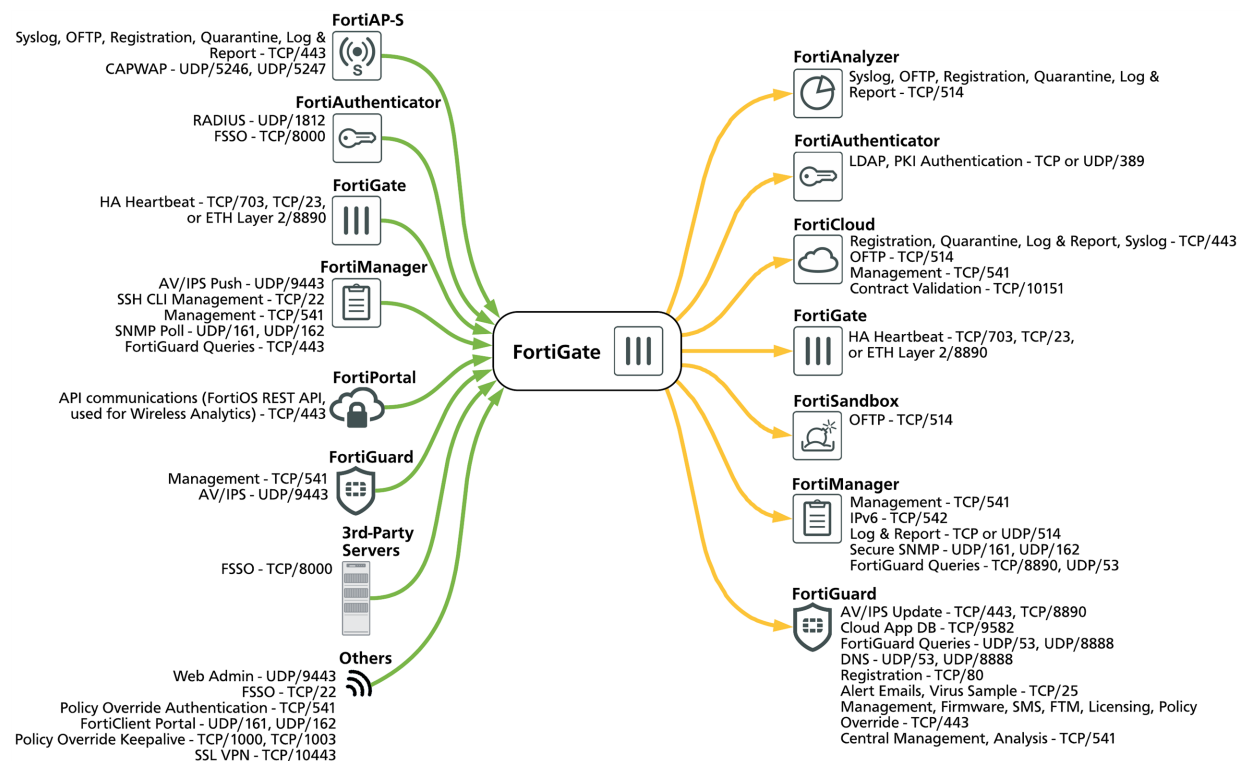
FortiOS ports and protocols

Communication to and from FortiOS is strictly controlled and only selected ports are opened for supported functionality such as administrator logins and communication with other Fortinet products or services.

Accessing FortiOS using an open port is protected by authentication, identification, and encryption requirements. As well, ports are only open if the feature using them is enabled.

FortiOS open ports

The following diagram and tables shows the incoming and outgoing ports that are potentially opened by FortiOS. For more details about open ports and the communication protocols that FortiOS uses, see the document [Fortinet Communication Ports and Protocols](#).



Incoming Ports

Purpose

Protocol/Port

FortiAP-S

Syslog, OFTP, Registration, Quarantine, Log & Report

TCP/443

CAPWAP

UDP/5246, UDP/5247

Incoming Ports		
Purpose		Protocol/Port
FortiAuthenticator	RADIUS	UDP/1812
	FSSO	TCP/8000
FortiGate	HA Heartbeat	TCP/703, TCP/23, or ETH Layer 2/8890
FortiGuard	Management	TCP/541
	AV/IPS	UDP/9443
FortiManager	AV/IPS Push	UDP/9443
	SSH CLI Management	TCP/22
	Management	TCP/541
	SNMP Poll	UDP/161, UDP/162
	FortiGuard Queries	TCP/443
FortiPortal	API communications (FortiOS REST API, used for Wireless Analytics)	TCP/443
Others	Web Admin	TCP/80, TCP/443
	FSSO	TCP/8000
	Policy Override Authentication	TCP/443, TCP/8008
	FortiClient Portal	TCP/8009
	Policy Override Keepalive	TCP/1000, TCP/1003
	SSL VPN	TCP/10443
3rd-Party Servers	FSSO	TCP/8000

Outgoing Ports		
Purpose		Protocol/Port
FortiAnalyzer	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
FortiAuthenticator	LDAP, PKI Authentication	TCP or UDP/389

Outgoing Ports		
Purpose		Protocol/Port
FortiCloud	Registration, Quarantine, Log & Report, Syslog	TCP/443
	OFTP	TCP/514
	Management	TCP/541
	Contract Validation	TCP/10151
FortiGate	HA Heartbeat	TCP/703, TCP/23, or ETH Layer 2/8890
FortiGuard	AV/IPS Update	TCP/443, TCP/8890
	Cloud App DB	TCP/9582
	FortiGuard Queries	UDP/53, UDP/8888
	DNS	UDP/53, UDP/8888
	Registration	TCP/80
	Alert Email, Virus Sample	TCP/25
	Management, Firmware, SMS, FTM, Licensing, Policy Override	TCP/443
	Central Management, Analysis	TCP/541
FortiManager	Management	TCP/541
	IPv6	TCP/542
	Log & Report	TCP or UDP/514
	Secure SNMP	UDP/161, UDP/162
	FortiGuard Queries	TCP/8890, UDP/53
FortiSandbox	OFTP	TCP/514



Note that, while a proxy is configured, FortiGate uses the following URLs to access the FortiGuard Distribution Network (FDN):

- update.fortiguard.net
- service.fortiguard.net
- support.fortinet.com

Closing open ports

You can close open ports by disabling the feature that opens them. For example, if FortiOS is not managing a FortiAP then the CAPWAP feature for managing FortiAPs can be disabled, closing the CAPWAP port.

The following sections of this document described a number of options for closing open ports:

- [Use local-in policies to close open ports or restrict access on page 23](#)
- [Disable unused protocols on interfaces on page 22](#)

Security best practices

This chapter describes some techniques and best practices that you can use to improve FortiOS security.

Install the FortiGate unit in a physically secure location

A good place to start with is physical security. Install your FortiGate in a secure location, such as a locked room or one with restricted access. A restricted location prevents unauthorized users from getting physical access to the device.

If unauthorized users have physical access, they can disrupt your entire network by disconnecting your FortiGate (either by accident or on purpose). They could also connect a console cable and attempt to log into the CLI. Also, when a FortiGate unit reboots, a person with physical access can interrupt the boot process and install different firmware.

Register your product with Fortinet Support

You need to register your Fortinet product with Fortinet Support to receive customer services, such as firmware updates and customer support. You must also register your product for FortiGuard services, such as up-to-date antivirus and IPS signatures. Register your product by visiting <https://support.fortinet.com>.

Keep your FortiOS firmware up to date

Always keep FortiOS up to date. The most recent version is the most stable and has the most bugs fixed and vulnerabilities removed.

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you register your FortiGate or FortiOS VM, download firmware updates from the support web site, <https://support.fortinet.com>.

Before you install any new firmware, be sure to follow these steps:

- Review the Release Notes for the latest firmware release.
- Review the [Supported Upgrade Paths](#) guide to determine the best path to take from your current version of FortiOS to the latest version.
- Back up the current configuration.

Only FortiGate administrators who have read and write privileges can upgrade the FortiOS firmware.

System administrator best practices

This section describes a collection of changes you can implement to make administrative access to the GUI and CLI more secure.

Disable administrative access to the external (Internet-facing) interface

When possible, don't allow administration access on the external (Internet-facing) interface.

To disable administrative access, go to **Network > Interfaces**, edit the external interface and disable HTTPS, PING, HTTP, SSH, and TELNET under **Administrative Access**.

From the CLI:

```
config system interface
  edit <external-interface-name>
    unset allowaccess
  end
```

Allow only HTTPS access to the GUI and SSH access to the CLI

For greater security never allow HTTP or Telnet administrative access to a FortiGate interface, only allow HTTPS and SSH access. You can change these settings for individual interfaces by going to **Network > Interfaces** and adjusting the administrative access to each interface.

From the CLI:

```
config system interface
  edit <interface-name>
    set allowaccess https ssh
  end
```

Require TLS 1.2 for HTTPS administrator access

Use the following command to require TLS 1.2 for HTTPS administrator access to the GUI:

```
config system global
  set admin-https-ssl-versions tlsv1-2
end
```

TLS 1.2 is currently the most secure SSL/TLS supported version for SSL-encrypted administrator access.

Re-direct HTTP GUI logins to HTTPS

Go to **System > Settings > Administrator Settings** and enable **Redirect to HTTPS** to make sure that all attempted HTTP login connections are redirected to HTTPS.

From the CLI:

```
config system global
  set admin-https-redirect enable
end
```


Change the HTTPS and SSH admin access ports to non-standard ports

Go to **System > Settings > Administrator Settings** and change the HTTPS and SSH ports.

You can change the default port configurations for HTTPS and SSH administrative access for added security. To connect to a non-standard port, the new port number must be included in the collection request. For example:

- If you change the HTTPS port to 7734, you would browse to `https://<ip-address>:7734`.
- If you change the SSH port to 2345, you would connect to `ssh admin@<ip-address>:2345`

To change the HTTPS and SSH login ports from the CLI:

```
config system global
    set admin-sport 7734
    set admin-ssh-port 2345
end
```

If you change to the HTTPS or SSH port numbers, make sure your changes do not conflict with ports used for other services.

Maintain short login timeouts

Set the idle timeout to a short time to avoid the possibility of an administrator walking away from their management computer and leaving it exposed to unauthorized personnel.

To set the administrator idle timeout, go to **System > Settings** and enter the amount of time for the **Idle timeout**. A best practice is to keep the default time of 5 minutes.

To set the administrator idle timeout from the CLI:

```
config system global
    set admintimeout 5
end
```

You can use the following command to adjust the grace time permitted between making an SSH connection and authenticating. The range can be between 10 and 3600 seconds, the default is 120 seconds (minutes). By shortening this time, you can decrease the chances of someone attempting a brute force attack from being successful. For example, you could set the time to 30 seconds.

```
config system global
    set admin-ssh-grace-time 30
end
```

Restrict logins from trusted hosts

Setting up trusted hosts for an administrator limits the addresses from where they can log into FortiOS. The trusted hosts configuration applies to all forms of administrative access including HTTPS, SSH, ping, and SNMP. When you identify a trusted host for an administrator account, FortiOS accepts that administrator's login only from one of the trusted hosts. A login, even with proper credentials, from a non-trusted host is dropped.

To identify trusted hosts, go to **System > Administrators**, edit the administrator account, enable **Restrict login to trusted hosts**, and add up to ten trusted host IP addresses.

To add two trusted hosts from the CLI:

```
config system admin
    edit <administrator-name>
        set trustedhost1 172.25.176.23 255.255.255.255
```

```
set trustedhost2 172.25.177.0 255.255.255.0
end
```

Trusted host IP addresses can identify individual hosts or subnets. Just like firewall policies, FortiOS searches through the list of trusted hosts in order and acts on the first match it finds. When you configure trusted hosts, start by adding specific addresses at the top of the list. Follow with more general IP addresses. You don't have to add addresses to all of the trusted hosts as long as all specific addresses are above all of the 0.0.0.0 0.0.0.0 addresses.

Set up two-factor authentication for administrators

FortiOS supports FortiToken and FortiToken Mobile 2-factor authentication. FortiToken Mobile is available for iOS and Android devices from their respective application stores.

Every registered FortiGate unit includes two trial tokens for free. You can purchase additional tokens from your reseller or from Fortinet.

To assign a token to an administrator, go to **System > Administrators** and select **Enable Two-factor Authentication** for each administrator.

Create multiple administrator accounts

Rather than allowing all administrators to access FortiOS with the same administrator account, you can create accounts for each person or each role that requires administrative access. This configuration allows you to track the activities of each administrator or administrative role.

If you want administrators to have different functions you can add different administrator profiles. Go to **System > Admin Profiles** and select **Create New**.

Modify administrator account lockout duration and threshold values

By default, the FortiGate sets the number of password retries at three, allowing the administrator a maximum of three attempts to log into their account before locking the account for a set amount of time.

Both the number of attempts (`admin-lockout-threshold`) and the wait time before the administrator can try to enter a password again (`admin-lockout-duration`) can be configured within the CLI.

To configure the lockout options:

```
config system global
  set admin-lockout-threshold <failed_attempts>
  set admin-lockout-duration <seconds>
end
```

The default value of `admin-lockout-threshold` is 3 and the range of values is between 1 and 10. The `admin-lockout-duration` is set to 60 seconds by default and the range of values is between 1 and 4294967295 seconds.

Keep in mind that the higher the lockout threshold, the higher the risk that someone may be able to break into the FortiGate unit.

Example:

To set the `admin-lockout-threshold` to one attempt and the `admin-lockout-duration` to a five minute duration before the administrator can try to log in again, enter the commands:

```
config system global
  set admin-lockout-threshold 1
  set admin-lockout-duration 300
end
```



If the time span between the first failed login attempt and the `admin-lockout-threshold` failed login attempt is less than `admin-lockout-duration`, the lockout will be triggered.

Rename the admin administrator account

You can improve security by renaming the admin account. To do this, create a new administrator account with the `super_admin` admin profile and log in as that administrator. Then go to **System > Administrators** and edit the admin administrator and change the **User Name**. Renaming the admin account makes it more difficult for an attacker to log into FortiOS.

Add administrator disclaimers

FortiOS can display a disclaimer before or after logging into the GUI or CLI (or both). In either case the administrator must read and accept the disclaimer before they can proceed.

Use the following command to display a disclaimer before logging in:

```
config system global
  set pre-login-banner enable
end
```

Use the following command to display a disclaimer after logging in:

```
config system global
  set post-login-banner enable
end
```

You can customize the replacement messages for these disclaimers by going to **System > Replacement Messages**. Select **Extended View** to view and edit the **Administrator** replacement messages.

From the CLI:

```
config system replacemsg admin pre_admin-disclaimer-text
config system replacemsg admin post_admin-disclaimer-text
```

Global commands for stronger and more secure encryption

This section describes some best practices for employing stronger and more secure encryption.

Turn on global strong encryption

Enter the following command to configure FortiOS to use only strong encryption and allow only strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS, SSH, TLS, and SSL functions.

```
config sys global
    set strong-crypto enable
end
```

Disable MD5 and CBC for SSH

In some cases, you may not be able to enable strong encryption. For example, your FortiGate may be communicating with a system that does not support strong encryption. With `strong-crypto` disabled you can use the following options to prevent SSH sessions with the FortiGate from using less secure MD5 and CBC algorithms:

```
config sys global
    set ssh-hmac-md5 disable
    set ssh-cbc-cipher disable
end
```

Disable static keys for TLS

You can use the following command to prevent TLS sessions from using static keys (AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256):

```
config sys global
    set ssl-static-key-ciphers disable
end
```

Require larger values for Diffie-Hellman exchanges

Larger Diffie-Hellman values result in stronger encryption. Use the following command to force Diffie-Hellman exchanges to use 8192 bit values (the highest configurable DH value).

```
config sys global
    set dh-params 8192
end
```

Disable sending Malware statistics to FortiGuard

By default FortiOS periodically sends encrypted Malware statistics to FortiGuard. The Malware statistics record Antivirus, IPS, or Application Control events. This data is used to improved FortiGuard services. The Malware statistics that are sent do not include any personal or sensitive customer data. The information is not shared with any external parties and is used in accordance with Fortinet's [Privacy Policy](#).

To disable sending Malware statistics to FortiGuard, enter the following command:

```
config system global
    set fds-statistics disable
end
```

Disable auto USB installation

If USB installation is enabled, an attacker with physical access to a FortiGate could load a new configuration or firmware on the FortiGate using the USB port. You can disable USB installation by entering the following from the CLI:

```
config system auto-install
    set auto-install-config disable
    set auto-install-image disable
end
```

Set system time by synchronizing with an NTP server

For accurate time, use an NTP server to set system time. Synchronized time facilitates auditing and consistency between expiry dates used in expiration of certificates and security protocols.

From the GUI go to **System > Settings > System Time** and select **Synchronize with NTP Server**. By default, this causes FortiOS to synchronize with Fortinet's FortiGuard secure NTP server.

From the CLI you can use one or more different NTP servers:

```
config system ntp
    set type custom
    set ntpsync enable
    config ntpserver
        edit 1
            set server <ntp-server-ip>
        next
        edit 2
            set server <other-ntp-server-ip>
    end
```

Enable password policies

Go to **System > Settings > Password Policy**, to create a password policy that all administrators must follow. Using the available options you can define the required length of the password, what it must contain (numbers, upper and lower case, and so on) and an expiry time.

Use the password policy feature to make sure all administrators use secure passwords that meet your organization's requirements.

Configure auditing and logging

For optimum security go to **Log & Report > Log Settings** enable **Event Logging**. For best results send log messages to FortiAnalyzer or FortiCloud.

From FortiAnalyzer or FortiCloud, you can view reports or system event log messages to look for system events that may indicate potential problems. You can also view system events by going to **FortiView > System Events**.

Establish an auditing schedule to routinely inspect logs for signs of intrusion and probing.

Encrypt logs sent to FortiAnalyzer/FortiManager

To keep information in log messages sent to FortiAnalyzer private, go to **Log & Report > Log Settings** and when you configure Remote Logging to FortiAnalyzer/FortiManager select **Encrypt log transmission**.

From the CLI.

```
config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
    set enc-algorithm high
end
```

Disable interfaces that not used

To disable an interface from the GUI, go to **Network > Interfaces**. Edit the interface to be disabled and set **Interface State** to **Disabled**.

From the CLI, to disable the port21 interface:

```
config system interface
    edit port21
        set status down
    end
```

Disable unused protocols on interfaces

You can use the `config system interface` command to disable unused protocols that attackers may attempt to use to gather information about a FortiGate unit. Many of these protocols are disabled by default. Using the `config system interface` command you can see the current configuration of each of these options for the selected interface and then choose to disable them if required.

```
config system interface
    edit <interface-name>
        set dhcp-relay-service disable
        set pptp-client disable
        set arpforward disable
        set broadcast-forward disable
        set l2forward disable
        set icmp-redirect disable
        set vlanforward disable
        set stpforward disable
        set ident-accept disable
        set ipmac disable
        set netbios-forward disable
        set security-mode none
        set device-identification disable
        set lldp-transmission disable
    end
```

Option	Description
dhcp-relay-service	Disable the DHCP relay service.
pptp-client	Disable operating the interface as a PPTP client.
arpforward	Disable ARP forwarding.
broadcast-forward	Disable forwarding broadcast packets.
l2forward	Disable layer 2 forwarding.
icmp-redirect	Disable ICMP redirect.
vlanforward	Disable VLAN forwarding.
stpforward	Disable STP forwarding.
ident-accept	Disable authentication for this interface. The interface will not respond to a connection with an authentication prompt.
ipmac	Disable IP/MAC binding.
netbios-forward	Disable NETBIOS forwarding.
security-mode	Set to <code>none</code> to disable captive portal authentication. The interface will not respond to a connection with a captive portal.
device-identification	Disable device identification.
lldp-transmission	Disable link layer discovery (LLDP).

Use local-in policies to close open ports or restrict access

You can also use local-in policies to close open ports or otherwise restrict access to FortiOS.

Close ICMP ports

Use the following command to close all ICMP ports on the WAN1 interface. The following example blocks traffic that matches the ICMP_ANY firewall service.

```
config firewall local-in-policy
edit 1
set intf wan1
set srcaddr all
set dstaddr all
set action deny
set service ICMP_ANY
```

```
    set schedule always
end
```

Close the BGP port

Use the following command to close the BGP port on the wan1 interface. The following example blocks traffic that matches the BGP firewall service.

```
config firewall local-in-policy
edit 1
    set intf wan1
    set srcaddr all
    set dstaddr all
    set action deny
    set service BGP
    set schedule always
end
```




FORTINET®



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.